

## AMENDMENTS TO THE CLAIMS

**Claim 1 (Currently Amended)** A communication apparatus for communicating with a server apparatus based on a server certificate, the communication apparatus comprising:

a revocation number obtainment unit operable to obtain a revocation number from a repository apparatus storing the revocation number, the revocation number being a criterion for judging validity of the server certificate;

a revocation number judgment unit operable to judge validity of the revocation number;

a revocation number storage unit operable to store the revocation number obtained by the revocation number obtainment unit;

an identification number reading unit operable to read, from the server certificate, an identification number that identifies the server certificate;

a certificate judgment unit operable to judge the validity of the server certificate by comparing the identification number that identifies the server certificate with the revocation number stored by the revocation number storage unit; and

a communication control unit operable to establish a communication with the server apparatus when the certificate judgment unit judges the server certificate to be valid, and operable to disconnect~~revoke~~ a communication with the server apparatus when the certificate judgment unit judges the server certificate not to be valid,

wherein the revocation number judgment unit judges the validity of the revocation number by comparing the revocation number with a past revocation number, the past revocation number being (i) obtained by the revocation number obtainment unit before the revocation number has been obtained, (ii) stored by the revocation number storage unit, and (iii) a criterion

for judging the validity of the server certificate, and

wherein, when the revocation number judgment unit judges the revocation number to be valid, the certificate judgment unit (i) judges whether or not the identification number that identifies the server certificate is smaller than the revocation number stored by the revocation number storage unit, (ii) judges that the server certificate is not valid when the identification number that identifies the server certificate is judged to be smaller than the revocation number stored by the revocation number storage unit, and (iii) judges that the server certificate is valid when the identification number that identifies the server certificate is judged to be equal to or larger than the revocation number stored by the revocation number storage unit.

**Claim 2 (Cancelled)**

**Claim 3 (Cancelled)**

**Claim 4 (Currently Amended)**      The communication apparatus according to ~~Claim 3~~ Claim 1, wherein the revocation number judgment unit further judges the validity of the revocation number stored by the revocation number storage unit by comparing an identification number of a repository certificate indicating validity of the repository apparatus with the revocation number stored by the revocation number storage unit.

**Claim 5 (Previously Presented)**      The communication apparatus according to Claim 4, wherein the revocation number judgment unit judges that the repository apparatus is valid when

the identification number of the repository certificate is equal to or larger than the revocation number stored by the revocation number storage unit.

**Claim 6 (Cancelled)**

**Claim 7 (Currently Amended)** The communication apparatus according to ~~Claim 6~~ Claim 1, wherein the revocation number judgment unit judges that the revocation number obtained by the revocation number obtainment unit is valid when the revocation number obtained by the revocation number obtainment unit is equal to or larger than the past revocation number stored by the revocation number storage unit.

**Claim 8 (Previously Presented)** A certificate issuing apparatus for issuing a server certificate indicating validity of a server apparatus, the certificate issuing apparatus comprising:

a revocation number storage unit operable to store a revocation number, the revocation number being a criterion for judging validity of the server certificate;

a revocation number update unit operable to update the revocation number stored by the revocation number storage unit to a number that is larger than an identification number of a server certificate to be revoked, the revocation number update unit updating the revocation number when being notified of the identification number of the server certificate to be revoked; and

an issuing unit operable to issue a new server certificate including an identification number indicating a value that is equal to or larger than the revocation number stored by the

revocation number storage unit,

wherein, when the revocation number update unit updates the revocation number, the issuing unit issues the new server certificate to another server apparatus that corresponds to a server certificate including an identification number indicating a value that is smaller than the updated revocation number.

**Claim 9 (Cancelled)**

**Claim 10 (Cancelled)**

**Claim 11 (Previously Presented)** The certificate issuing apparatus according to Claim 8, further comprising an expiration date revocation number update unit operable to specify an identification number of a server certificate, specify an approaching expiration date, and update the revocation number stored by the revocation number storage unit to a number that is larger than the specified identification number of the server certificate.

**Claim 12 (Previously Presented)** The certificate issuing apparatus according to Claim 11, wherein, when the expiration date revocation number update unit updates the revocation number stored by the revocation number storage unit, the issuing unit issues the new server certificate to a server apparatus with a server certificate that is assigned an identification number that is smaller than the revocation number updated by the expiration date revocation number update unit.

**Claim 13 (Currently Amended)** A communication system comprising:

a server apparatus;

a certificate issuing apparatus for issuing a server certificate indicating validity of the server apparatus; and

a communication apparatus for communicating with the server apparatus based on the server certificate,

wherein the certificate issuing apparatus includes:

a first revocation number storage unit operable to store a revocation number, the revocation number being a criterion for judging validity of the server certificate;

a revocation number update unit operable to update the revocation number stored by the first revocation number storage unit to a number that is larger than an identification number of a server certificate to be revoked, the revocation number update unit updating the revocation number when being notified of the identification number of the server certificate to be revoked; and

an issuing unit operable to issue a new server certificate including an identification number indicating a value that is equal to or larger than the revocation number stored by the first revocation number storage unit,

wherein, when the revocation number update unit updates the revocation number, the issuing unit issues the new server certificate to another server apparatus that corresponds to a server certificate including an identification number indicating a value that is smaller than the updated revocation number,

wherein the communication apparatus includes:

a revocation number obtainment unit operable to obtain a revocation number from a repository apparatus storing the revocation number, the revocation number being a criterion for judging the validity of the server certificate;

a revocation number judgment unit operable to judge validity of the revocation number;

a second revocation number storage unit operable to store the revocation number obtained by the revocation number obtainment unit;

an identification number reading unit operable to read, from the server certificate, an identification number that identifies the server certificate;

a certificate judgment unit operable to judge the validity of the server certificate by comparing the identification number that identifies the server certificate with the revocation number stored by the second revocation number storage unit; and

a communication control unit operable to establish a communication with the server apparatus when the certificate judgment unit judges the server certificate to be valid, and operable to ~~revoke~~ disconnect a communication with the server apparatus when the certificate judgment unit judges the server certificate not to be valid, ~~and~~

wherein the revocation number judgment unit judges the validity of the revocation number by comparing the revocation number with a past revocation number, the past revocation number being (i) obtained by the revocation number obtainment unit before the revocation number has been obtained, (ii) stored by the revocation number storage unit, and (iii) a criterion for judging the validity of the server certificate, and

wherein, when the revocation number judgment unit judges the revocation number to be valid, the certificate judgment unit (i) judges whether or not the identification number that identifies the server certificate is smaller than the revocation number stored by the second revocation number storage unit, (ii) judges that the server certificate is not valid when the identification number that identifies the server certificate is judged to be smaller than the revocation number stored by the second revocation number storage unit, and (iii) judges that the server certificate is valid when the identification number that identifies the server certificate is judged to be equal to or larger than the revocation number stored by the second revocation number storage unit.

**Claim 14 (Currently Amended)** A communication method of communicating with a server apparatus based on a server certificate, the communication method comprising:

obtaining a revocation number from a repository apparatus storing the revocation number, the revocation number being a criterion for judging validity of the server certificate;  
judging validity of the revocation number;

storing the revocation number obtained by the obtaining of the revocation number into a recording unit;

reading, from the server certificate, an identification number that identifies the server certificate;

judging the validity of the server certificate by comparing the identification number read by the reading of the identification number with the revocation number stored by the recording unit; and

establishing a communication with the server apparatus when the judging of the validity of the server certificate judges that the server certificate is valid, and ~~revoking~~ disconnecting a communication with the server apparatus when the judging of the validity of the server certificate judges that the server certificate is not valid,

wherein the judging of the validity of the revocation number judges the validity of the revocation number by comparing the revocation number with a past revocation number, the past revocation number being (i) obtained by the obtaining before the revocation number has been obtained, (ii) stored by the storing, and (iii) a criterion for judging the validity of the server certificate, and

wherein, when the revocation number is judged to be valid by the judging of the validity of the revocation number, the judging of the validity of the server certificate judges whether or not the identification number that identifies the server certificate is smaller than the revocation number stored in the recording unit, judges that the server certificate is not valid when the identification number that identifies the server certificate is judged to be smaller than the revocation number stored in the recording unit, and judges that the server certificate is valid when the identification number that identifies the server certificate is judged to be equal to or larger than the revocation number stored in the recording unit.

**Claim 15 (Previously Presented)** A certificate issuing method of issuing a server certificate indicating validity of a server apparatus, the certificate issuing method comprising:

storing, into a recording unit, a revocation number, the revocation number being a criterion for judging validity of the server certificate;

updating the revocation number stored by the storing of the revocation number to a number that is larger than an identification number of a server certificate to be revoked, the updating of the revocation number being performed upon being notified of the identification number of the server certificate to be revoked; and

issuing a new server certificate including an identification number indicating a value that is equal to or larger than the revocation number stored by the storing of the revocation number,

wherein, when the updating of the revocation number updates the revocation number, the new server certificate is issued to another server apparatus that corresponds to a server certificate including an identification number indicating a value that is smaller than the updated revocation number.

**Claim 16 (Currently Amended)** A computer-readable recording medium having a program recorded thereon, the program for communicating with a server apparatus based on a server certificate, the program causing a computer to execute a method comprising:

obtaining a revocation number from a repository apparatus storing the revocation number, the revocation number being a criterion for judging validity of the server certificate;

judging validity of the revocation number;

storing the revocation number obtained by the obtaining of the revocation number into a recording unit;

reading, from the server certificate, an identification number that identifies the server certificate;

judging the validity of the server certificate by comparing the identification number read

by the reading of the identification number with the revocation number stored by the recording unit; and

establishing a communication with the server apparatus when the judging of the validity of the server certificate judges that the server certificate is valid, and ~~revoking disconnecting~~ a communication with the server apparatus when the judging of the validity of the server certificate judges that the server certificate is not valid,

wherein the judging of the validity of the revocation number judges the validity of the revocation number by comparing the revocation number with a past revocation number, the past revocation number being (i) obtained by the obtaining before the revocation number has been obtained, (ii) stored by the storing, and (iii) a criterion for judging the validity of the server certificate, and

wherein, when the revocation number is judged to be valid by the judging of the validity of the revocation number, the judging of the validity of the server certificate judges whether or not the identification number that identifies the server certificate is smaller than the revocation number stored in the recording unit, judges that the server certificate is not valid when the identification number that identifies the server certificate is judged to be smaller than the revocation number stored in the recording unit, and judges that the server certificate is valid when the identification number that identifies the server certificate is judged to be equal to or larger than the revocation number stored in the recording unit.

**Claim 17 (Previously Presented)** A computer-readable recording medium having a program recorded thereon, the program for issuing a server certificate indicating validity of a server

apparatus, the program causing a computer to execute a method comprising:

storing, into a recording unit, a revocation number, the revocation number being a criterion for judging validity of the server certificate;

updating the revocation number stored by the storing of the revocation number to a number that is larger than an identification number of a server certificate to be revoked, the updating of the revocation number being performed upon being notified of the identification number of the server certificate to be revoked; and

issuing a new server certificate including an identification number indicating a value that is equal to or larger than the revocation number stored by the storing of the revocation number,

wherein, when the updating of the revocation number updates the revocation number, the new server certificate is issued to another server apparatus that corresponds to a server certificate including an identification number indicating a value that is smaller than the updated revocation number.